6-18-2013

Modelling Organizational Resilience in the Cloud

Andrea Herrera
University of Auckland, anhesue@gmail.com

Lech Janczewski
University of Auckland, lech@auckland.ac.nz

MODELLING ORGANISATIONAL RESILIENCE IN THE CLOUD

Andrea Herrera, Department of Information Systems & Operations Management, University of Auckland, New Zealand, a.herrera@auckland.ac.nz

Lech Janczewski, Department of Information Systems & Operations Management, University of Auckland, New Zealand, l.janczewski@auckland.ac.nz

Abstract

Cloud computing (CC) is a promising information and communication technologies (ICT) services delivery model that has already had a significant impact on Government agencies, small and medium enterprises and large organisations. Even though its adoption is moving from the early stage to mainstream, many organisations are still afraid that their resilience might deteriorate because of the additional levels of abstraction that CC introduces. This additional complexity makes the assessment of ICT operational resilience more difficult and no consensus exists of such analysis. Following a multi-method approach, this research proposal first extends prior research in the field, looking at new possible categories of resilience-oriented requirements when working in CC environments. Based on the results, this research will propose a conceptual model that helps organisations to maintain and improve Organisational Resilience (OR) when working in CC environments, from the ICT operational perspective. Particularly, as a lack of coordination has been identified as one of the main problems when facing disruptive incidents, using coordination theory, this research will identify the fundamental coordination processes involved in the proposed model. The results of this research should be of interest to academic researchers and practitioners.

Keywords: cloud computing, ICT resilience, conceptual modelling, coordination theory.

1 INTRODUCTION

Cloud computing (CC) is a new paradigm that promises uncountable benefits for organisations including agility, reduced time to market, reduced cost and renewed focus on the core business. According to IDC[1], regardless of their specific motivation, organisations are increasingly turning to this type of service; in fact, it has been predicted that by 2016, US $1 of every US $5 will be spent on cloud-based software and infrastructure (Mahowald & Sullivan, 2012). However, like every new trend, CC also has risks and concerns that are being identified in order to use it effectively and safely. An increasing number of researchers and practitioners worldwide are developing new knowledge about CC in a wide range of applications from the business perspective to more technical issues (Yang & Tate, 2012). In the former, researchers have been working specifically on economic impact, costs, reasons for adoption and growth trends (Centre for Economics and Business Research Ltd, 2011; Iansiti & Richards, 2011; Marston et al., 2011; Saya et al., 2010). In the latter, issues regarding portability, interoperability and security have been studied (Buyya et al., 2010; Catteddu & Hogben, 2009; Chen et al., 2010; Cloud Security Alliance, 2010).

Somewhere in the intersection between these technical and business concerns, many researchers and renowned international organisations and associations have identified *Availability / Business Continuity* as one of the main obstacles to and opportunities for the growth of CC (Armbrust et al., 2010; Badger et al., 2012; Catteddu & Hogben, 2009; Cloud Security Alliance, 2011; Hancock & Hutley, 2012). Business continuity and disaster recovery plans become even more important in cloud environments because cloud outages and cloud security compromises are some of the many additional issues that can lead to an operational disruption. Thus, if things go wrong, a joint effort between the cloud provider and the organisation that requires high levels of coordination, is needed in order to avoid unacceptable downtimes (Toomer, 2011).

According to the International Organization for Standardization (ISO), Business Continuity Management (BCM) is an "holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which *provides a framework for building organizational resilience* (…)" (2012, p. 2). Then, the final objective of BCM is to build Organisational Resilience (OR). In fact, this concept has gained considerable attention in the last few years, mainly because organisations are the engine of economic growth and sustainable development and disruptions can have significant and widespread impacts globally (Boin & Lagadec, 2000). On top of that, the annual number of both natural and man-made disasters has increased significantly during the past 20 years. As a consequence, the need for organisations to exhibit high reliability in the face of adversity has increased and in order to build and improve OR a deep understanding of the information and communication technologies (ICT) environment is essential. These two factors, the massive adoption of CC as a model for performing ICT functions and the growing relevance of the OR concept, have heightened the need to strengthen the ability of organisations to respond to disruptive incidents when working in cloud environments.

Based on these facts, this research aims, firstly, to understand how the adoption of CC impacts the ability of an organisation to continue to function in the face of disruption, in order to identify new categories of resilience-oriented requirements when working in CC environments. Secondly, using these results and the analysis of the CC reference architecture (Liu et al., 2011) the main purpose of this research is to propose a conceptual model that helps organisations to maintain and improve OR when working in CC environments, from the ICT operational perspective. In addition, as lack of coordination has been identified as one of the main problems when facing disruptive incidents (Hossain & Kuti, 2010). Thirdly, using coordination theory (Malone & Crowston, 1994) this research will identify the fundamental coordination processes involved in the proposed model. The assessment of these two artefacts will be performed through the experts' opinions approach, and walkthrough and tabletop exercises. Finally, the proposed artefacts will be used to analyse one of the current ICT

[1] International Data Corporation is a market research specialized in information technology.

resilience standards in order to identifying possible gaps and make some suggestions to respond to the new CC requirements. It is expected that the designed artefacts will integrate the foundational and practical requirements of ICT operational resilience in CC environments and could be used for planning and decision making to anticipate, prevent, prepare for, and respond to ICT disruptive incidents.

2 LITERATURE REVIEW AND RESEARCH QUESTIONS

In seeking to understand the impact of CC adoption in OR, firstly this section gives a brief description of CC and its main characteristics. Secondly, it presents a broad overview related to the resilience concept focusing on OR and how coordination among individuals, ICT services and organisations is an essential process especially when responding to disruptive incidents. Thirdly, it gives an overview of some well cited studies conducted in OR that focus on the domain of ICT and lastly, it presents the primary research questions for this research.

2.1 Cloud computing as an ICT performing functions model

CC is a type of computing based on the delivery of services. There are many definitions but there is broad acceptance of the one provided by the US National Institute for Standards and Technology (NIST). NIST defines it as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2009, p. 2). This definition requires computing services to be accessible across private or public networks and also implies that computing resources are pooled, reusable and rapidly reconfigured. Therefore, five essential characteristics are derived: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. In practice CC describes three predominant and related service models (Hancock & Hutley, 2012):

- SaaS - Software as a Service or paying access to software as web-accessed services instead of installing it on the premises.
- PaaS - Platform as a Service or developing and hosting tailor made software in cloud environments (platforms) that provide all required tools, languages, databases and resources.
- IaaS - Infrastructure as a Service or paying access to a computer processing power and storage.

In addition, there are four deployment models for these cloud service offerings: public, private, community and hybrid. The main characteristics of each of them and their main benefits are summarized in Table 1 below.

Despite the benefits there are several constraints that need to be overcome (Armbrust et al., 2010; Hancock & Hutley, 2012; Intelligence and National Security Alliance, 2012). The natural barriers to full adoption include, but are not limited to:

- Speed/latency issues and reliance on telecommunications services providers.
- Compatibility of an organisation's internal processes with cloud offerings.
- Location of data and related security and data sovereignty issues.
- Business continuity/disaster recovery and integration**.**
- Limited knowledge of product offering and lack of familiarity of business with opportunities.

Business continuity and disaster recovery plans become even more important in CC environments because cloud outages and cloud security compromises are some of the many additional issues that can lead to an operational disruption.

Cloud type	Definitions from (Liu et al., 2011, pp. 10-12)	**Benefits** (Armbrust et al., 2010; Hancock & Hutley, 2012; Intelligence and National Security Alliance, 2012)
Public	"A public cloud is one in which the cloud infrastructure and computing resources are made available to the general public over a public network".	* Ability to rapidly scale the allocation of computing resources to match fluctuations in business demand. * Utility-based pricing, then users only pay for computing resources actually used. * Potentially large economies of scale.
Private	"A private cloud gives a single cloud consumer's organization the exclusive access to and usage of the infrastructure and computational resources".	* Considered the most secure option but with reduced potential for economies of scale and productivity gains.
Community	"A community cloud serves a group of cloud consumers which have shared concerns such as mission objectives, security, privacy, and compliance policy (…) It is considered the half way between private and public clouds".	* Reduced economies of scale traded- off for increased security.
Hybrid	"A hybrid cloud is a composition of two or more clouds that remain as distinct entities but are bound together by standardized or proprietary technology that enables data and application portability".	* Allows for multiple deployment methods to meet specific business/agency needs.

Table 1. Cloud deployment models – Characteristics and benefits

2.2 Organisation resilience and coordination processes

Resilience may be viewed as a property or quality that enables a system (individual, organisation or community) to adapt and recover from a disturbance. Notwithstanding the many definitions in the literature, researchers recognise two general types: engineering resilience and ecological resilience (Holling, 2010); the main difference being that the former focuses on efficiency while the latter focuses on persistence. In the field of management, OR emerged in literature in the 1990s as an explanation for the ability of organisations to survive and also thrive when exposed to external shocks such as natural disasters, terrorist attacks and uncertain environments (Wilson, 2010). The concept has been applied to crisis management, disasters and high-reliability organisations (HROs) (Coutu, 2002; Dalziell & McManus, 2004; Kendra & Wachtendorf, 2003; Paton & Johnston, 2001; Stephenson, 2010; Tierney, 2003; Weick & Sutcliffe, 2001; Weick et al., 2008; Woods & Wreathall, 2008). Particularly, Dalziell and McManus (2004) have identified that from this perspective, the main implications of each of the two recognised types of resilience are:

- Engineering resilience implies "maximising the efficiency of systems and process to return and maintain the system at its desired state" (p. 8).
- Ecological resilience implies "designing flexible systems and processes that continue to function in the face of disturbances" (p. 8).

Moreover, organisations increasingly depend on partnerships to achieve their mission (Caralli et al., 2010). External partners provide essential skills and functions as in the case of CC, where organisations that are consuming CC services are ceding control of some of their business processes to their CC provider. Therefore, organisations are forced to rethink how to assess and build their OR and, especially under suddenly altered conditions of operation, when the coordination process among individuals, ICT services, and other organisations is particularly complex and not well-understood (Comfort & Kapucu, 2006). In fact, Hossain and Matthew (2010) highlight that many of the underlying problems during a disruptive incident response are the result of a poor coordination process. In addition, coordination has been studied in both stable working relationships (Malone & Crowston, 1994) and disruptive incidents response (Comfort & Kapucu, 2006; Hossain & Kuti, 2010). In the former, the main processes analysed include managing shared resources, producer/consumer

relationships, simultaneity constraints, and tank/subtask dependencies while in the latter, a social networking and a complex adaptive systems perspective have been explored for overcoming coordination problems in emergency response networks.

Based on the abovementioned findings, this study also seeks to extend the scope of prior research by looking at the main changes in the partnership coordination processes when handling disruptive incidents and by adopting an ecological resilience approach in order to focus on designing flexible coordination processes between organisations consuming cloud services and their cloud providers.

2.3 Organisational resilience in ICT

In the context of ICT, resilience has been studied mainly from two different perspectives. The first perspective is essentially technical and is often used as a synonym of robustness or fault tolerance. Thus, failures are unavoidable and a resilient system is capable of operating in perturbed mode (Bursztein & Goubault-Larrecq, 2007; Hawes & Reed, 2006; Najjar & Gaudiot, 1990). The second perspective is organisational, being the main interest of this research, and has been studied mainly to understand: how computing systems impact organisational performance, how to assess alternative methods and how to establish essential components. A brief summary of research addressing these topics is presented in Table 2.

Topic	Authors
How the strengthen of information systems (individual and systems level) is translated into reliable organisational performance	(Butler & Gray, 2006; Riolli & Savicki, 2003; Shao, 2005)
Impact of information technology and managerial pro-activeness in building net-enabled organisational resilience	(Oh & Teo, 2006)
Comparison of different contingency plans or resilience scenarios, trade-offs and decision	(Post & Diltz, 1986; Van de Walle & Rutkowski, 2006; Zobel, 2011; Zobel & Khansa, 2012)
Establishment of the essential components of disaster recovery methods	(Cumbie, 2007) (Mousavi et al., 2012)
Resilience Management Model (RMM) that seeks to manage of ICT operational resilience across three disciplines: security management, BCM and ICT operations management.	(Caralli et al., 2010)

Table 2. ICT organisational resilience-related research

However, few academics and practitioner associations have published specific research on how the adoption of CC impacts the ICT operational resilience and, in general, how to maintain and improve OR when working in cloud environments. Some of these are briefly outlined below:

- Kounev et al. (2012) define resilience as the "system's ability to continue providing available, responsive and reliable services under external perturbations such as security attacks, accidents, unexpected load spikes or fault-loads" (p. 67). The author's consider resilience as part of dependability and provide an overview of the research challenges and opportunities in providing dependability and resilience in cloud environments mainly from the self-adaptive and power management perspectives.
- Undheim, Chilwan and Heegaard (2011) focus on the availability attribute of a cloud service level agreement (SLA). They develop a simplified cloud system model and identify two possible dimensions for differentiating cloud application as well as proposing some important improvements to the cloud's SLAs.
- The Cloud Security Alliance (2011) has been working in the Cloud Controls Matrix, a security controls framework for cloud providers and consumers in assessing the overall security risk of a cloud provider. The domain called "Resiliency" addresses aspects like BCM policy, Impact Analysis, BCM testing and some specific mechanism for particular failures.

This shows that research in ICT operational resilience in CC environments is relatively unexplored and a recent academic literature review shows that many, if not all, avenues are open for future research in this topic (Hoberg et al., 2012).

2.4 Research questions

CC has already had a significant impact on Government agencies, small and medium enterprises and large organisations (Lansiti & Richards, 2011). According to the IDC ICT cloud services are moving from the early stage of adoption to the mainstream adoption (Gens, 2010), however, organisations are still afraid that their resilience might deteriorate because the additional levels of abstraction that CC introduces makes the assessment of ICT operational resilience more difficult (Da Rold et al., 2011) and no consensus yet exists on the form or content of such analysis. Based on this, it is the interest of this study to find out what the requirements are for setting up and managing an effective ICT operational resilience management system in CC environments and four research questions around this issue have been identified:

- RQ1: what are the controls and coordination mechanisms that organisations, working in cloud environments, currently use to handle disruptive incidents? An exploratory study will be conducted in order to identify new categories of resilience-oriented requirements when working in CC environments.
- RQ2: how do the main reference architecture characteristics of CC affect the ICT operational resilience requirements? What new requirements emerge? This part of the study will look at the reference architecture components of CC and mapping them with the current ICT resilience management requirements in order to identify possible gaps.

As a result of this first part, this research will propose a conceptual model that helps organisations to maintain and improve OR when working in CC environments, from the ICT operational perspective, focusing on the coordination processes involved in the model. Following, in order to improve the effectiveness of the ICT resilience programs in organisations working in cloud environments an answer to the two final questions of this study needs to be found. Therefore, the proposed artefacts will be used to analyse one of the current ICT resilience standards in order to identify possible gaps and contribute suggestions to respond to the new CC requirements and thereby providing answers to the two final questions.

- RQ3: what should be amended in the current ICT resilience / BCM standards to fulfil these new needs?
- RQ4: in order to support these standards, how should the current controls/processes be adjusted? What new controls/processes should be created?

3 RESEARCH DESIGN

In the field of information systems many research methodologies have been used, depending on the topic and the philosophical position of the researchers (Burstein & Gregor, 1999). The specific topic that this research is addressing has two main scientific interests. On one hand, it aims to understand how the adoption of CC impacts the OR requirements in order to identify and classify categories of mechanisms that are being used by organisations consuming CC services. This part of the research pursues fundamentally a knowledge-producing objective. On the other hand, it also aims to propose a model that helps organisations that are turning to CC services to maintain and improve their OR from the ICT operational perspective, which is fundamentally a knowledge-using objective. Therefore, the dual nature of the addressed problem is clearly recognisable and this research aims to solve a practical problem while contributing to the body of knowledge. In addition, given the social-technical nature of the problem: “joint effort between the cloud provider and the organisation that requires high levels of coordination in order to avoid unacceptable downtimes”, primarily an interpretive approach is employed.

In addition, a number of studies have found that a multiple research methodology should be used to discover different dimensions of the research problem, particularly when the problem deals with real-

world complexities, in order to achieve richer results (Adams & Courtney, 2004; Mingers, 2001; Nunamaker et al., 1991). Based on the above, this research adopts the multi-methodological approach proposed by Mingers (2001) that follows four major phases: appreciation, analysis, assessment and action as shown in the Figure 1 below:

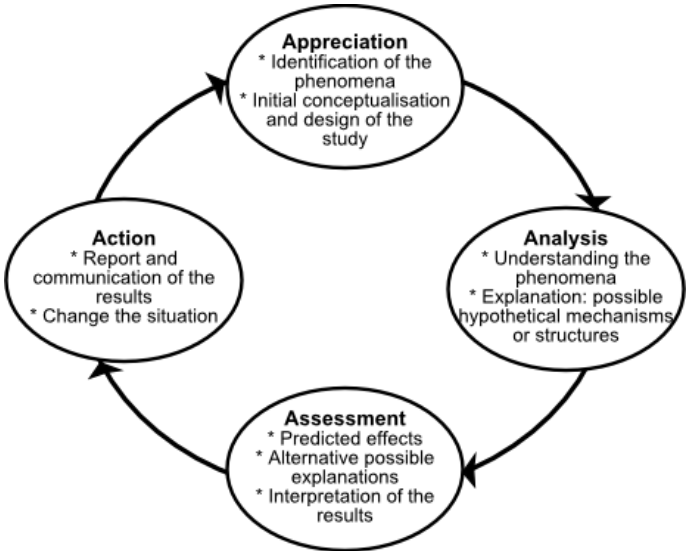

Figure 1. Research as a Process: a Multi-method Approach to IS Research, based on (Mingers, 2001, pp. 245-246)

Specifically, this research in progress proposal is structured as follows:

- The appreciation phase will organise the exploratory study and aims to identify new categories of resilience-oriented requirements when working in CC environments. Collection of real-world data through semi-structured interviews will help to identify and classify the specific mechanisms that are being used by organisations consuming CC services.
- The phase of analysis, using the results from the previous phase and focusing on the reference architecture of CC (Liu et al., 2011), will propose a conceptual model that helps organisations to maintain and improve OR when working in CC environments from the ICT operational perspective. In addition, as lack of coordination has been identified as one of the main problems when facing disruptive incidents, this model will include the fundamental coordination processes for overcoming managing dependencies problems between the organisation that is consuming cloud services and its CC provider.
- The assessment phase will test the two designed artefacts through three different approaches: first, based on a structuralist approach the elements of the model and the connections among them will be assessed. Secondly, following an experts' opinions approach the two artefacts will be presented to determine the quality of their foundation in order to obtain academic judgments as an additional input to refine it. Finally, in order to demonstrate the validity of the artefacts through different types of tests, like walkthrough and tabletop exercises, that are domain specific to the main research topic, ICT resilience.
- In the final action phase the proposed artefacts will be used to analyse one of the current ICT resilience standards in order to identifying possible gaps and make some suggestions to respond to the new CC requirements.

In addition, other authors have proposed conceptual frameworks for understanding, executing and evaluating IS research when using multiple paradigms. For instance, the framework proposed by Hevner et al (2004) is particularly helpful for this study because it addresses the "interplay among business strategy, IT strategy, organizational infrastructure, and IS infrastructure" (p. 78) while balancing the practical and theoretical contributions. In conclusion, this study is employing mainly an interpretive approach adopting a tailored multi-method framework.

4 EXPECTED CONTRIBUTIONS

The mains contribution of this study will be the proposed conceptual model and the fundamental coordination processes involved in the model. It is expected that the designed artefacts will integrate the foundational and practical requirements of ICT operational resilience in CC environments and be used for planning and decision making to anticipate, prevent, prepare for, and respond to ICT disruptive incidents. Thus, the results of this research should be of interest to academic researchers and practitioners.

In addition, given the explained context and the problem addressed, this research tangentially contributes to:

- Establishing a common terminology in ICT resilience that could be used for both academics and practitioners to facilitate its understanding and/or its operationalization. Particularly, from the CC services market perspective, the current lack of common terminology in ICT operational resilience is a specific problem that makes it more difficult to assess the trustworthiness of CC providers as mentioned previously.
- Identifying and classifying new requirements in the ICT resilience subject for cloud environments that could guide future research. Also, this classification could be used as an educational material to improve resilience awareness in organisations working in cloud environments.
- Identifying controls and mechanisms that organisations could use to minimise potential impacts of ICT services disruptions particularly useful for cloud environments. Even though current ICT resilience standards provide guideline that can be used by organisations to achieve this objective, new specific requirements for cloud environments could demand some changes.
- Reducing CC adoption barriers, working on and learning from one of the identified challenges. This research supports the boosting of cloud computing and its positive impacts and helps with increasing resilience against the risks that ICT can bring to organisations (World Economic Forum & INSEAD, 2012).
- Enabling reliable services, organisations using CC can expand their markets and governments can make their services more efficient while decreasing ICT expenses but not their reliability (European Commision, 2012).

ACKNOWLEDGMENTS

A special thank you goes to Dr. Fernando Beltrán and Dr. David Sundaram for their valuable comments and sharing their knowledge.

References

Adams, L. A., & Courtney, J. F. (2004, 5-8 Jan. 2004). *Achieving relevance in IS research via the DAGS framework.* Paper presented at the System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on System Sciences.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., . . . Zaharia, M. (2010). A view of cloud computing. *Commun. ACM, 53*(4), 50-58. doi: 10.1145/1721654.1721672

Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2012). *SP 800-146: Cloud Computing Synopsis and Recommendations*. Retrieved from http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

Boin, A., & Lagadec, P. (2000). Preparing for the Future: Critical Challenges in Crisis Management. *Journal of Contingencies and Crisis Management, 8*(4), 185-191. doi: 10.1111/1468-5973.00138

Burstein, F., & Gregor, S. (1999). *The systems development or engineering approach to research in information systems: an action research perspective.*, 10th Australasian Conference on Information Systems.

Bursztein, E., & Goubault-Larrecq, J. (2007). A logical framework for evaluating network resilience against faults and attacks. *Advances in Computer Science–ASIAN 2007. Computer and Network Security*, 212-227.

Butler, B. S., & Gray, P. H. (2006). Reliability, mindfulness, and information systems [Article]. *MIS Quarterly, 30*(2), 211-224.

Buyya, R., Ranjan, R., & Calheiros, R. (2010). InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services. In C.-H. Hsu, L. Yang, J. Park & S.-S. Yeo (Eds.), *Algorithms and Architectures for Parallel Processing* (Vol. 6081, pp. 13-31): Springer Berlin / Heidelberg.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). *CERT® Resilience Management Model v1.0: Improving Operational Resilience Processes* (CMU/SEI-2010-TR-012
ESC-TR-2010-012): Carnegie Mellon

Catteddu, D., & Hogben, G. (2009). *Cloud Computing: Benefits, risks and recommendations for information security*: European Network and Information Security Agency. Retrieved from http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Centre for economics and business research ltd. (2011). *The cloud dividend: Part Two - The economic benefits of cloud computing to business and the wider EMEA economy (Comparative analysis of the impact on aggregated industry sectors)*. London: Cebr. Retrieved from http://www.globbtv.com/microsite/35/Adjuntos/CLOUD-DIVIDEND-REPORT.PDF

Chen, Y., Paxson, V., & Katz, R. H. (2010). *What's New About Cloud Computing Security?* (UCB/EECS-2010-5): University of California at Berkeley - Electrical Engineering and Computer Sciences. Retrieved from http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

Cloud Security Alliance. (2010). *Top threats to cloud computing, version 1.0.* Retrieved from http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Cloud Security Alliance. (2011). *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*. Retrieved from https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Comfort, L. K., & Kapucu, N. (2006). Inter-organizational coordination in extreme events: The World Trade Center attacks, September 11, 2001. *Natural Hazards, 39*(2), 309-327.

Coutu, D. L. (2002). How resilience works. *Harvard Business Review, 80*(5), 46-56.

Cumbie, B. (2007). *The Essential Components of Disaster Recovery Methods: A Delphi Study Among Small Businesses*. Paper presented at the AMCIS 2007 Proceedings. Paper 115.

Da Rold, C., Heiser, J., & Morency, J. P. (2011). The Realities of Cloud Services Downtime: What You Must Know and Do. Retrieved from

Dalziell, E., & McManus, S. (2004). *Resilience, Vulnerability and Adaptive Capacity: Implications for System Performance*. Paper presented at the International Forum for Engineering Decision Making.

European Commision. (2012). *Unleashing the Potential of Cloud Computing in Europe*. Brussels: Retrieved from http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf.

Gens, F. (2010). *IDC IT Cloud Services Survey, 2Q10*

Hancock, I., & Hutley, N. (2012). *Modelling the Economic Impact of Cloud Computing*: KPMG and Australian Information Industry Association (AIIA). Retrieved from http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/modelling-economic-impact-cloud-computing.pdf

Hawes, C., & Reed, C. (2006). Theoretical steps towards modelling resilience in complex systems. *Computational Science and Its Applications-ICCSA 2006*, 644-653.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Q., 28*(1), 75-105.

Hoberg, P., Wollersheim, J., & Krcmar, H. (2012). *The Business Perspective on Cloud Computing - A Literature Review of Research on Cloud Computing*. Paper presented at the AMCIS 2012 Proceedings. Paper 5.

Holling, C. S. (2010). Engineering resilience versus ecological resilience. In L. H. Gunderson, C. R. Allen & C. S. Holling (Eds.), *Foundations of ecological resilience* Washington : Island Press, c2010.

Hossain, L., & Kuti, M. (2010). Disaster response preparedness coordination through social networks. *Disasters, 34*(3), 755-786.

Iansiti, M., & Richards, G. L. (2011). *Economic Impact of Cloud Computing White Paper*. Working papers series. Retrieved from http://ssrn.com.ezproxy.auckland.ac.nz/abstract=1875893

Intelligence and National Security Alliance. (2012). *Cloud Computing: Risk, Benefits, and Mission Enhancement for the Intelligence Community*: Intelligence and National Security Alliance - INSA, Cloud Computing task force. Retrieved from http://www.insaonline.org/assets/files/White%20Papers/INSA_Cloud_Computing_2012_FINAL.pdf

International Organization for Standardization. (2012). 22301: Societal security - Business continuity management systems - Requirements *Terms and Definitions*. Switzerland.

Kendra, J. M., & Wachtendorf, T. (2003). Elements of resilience after the world trade center disaster: reconstituting New York City's Emergency Operations Centre. *Disasters, 27*(1), 37-53.

Kounev, S., Reinecke, P., Brosig, F., Bradley, J., Joshi, K., Babka, V., . . . Gilmore, S. (2012). Providing Dependability and Resilience in the Cloud: Challenges and Opportunities. In K. Wolter (Ed.), *Resilience assessment and evaluation of computing systems*: Berlin ; London : Springer, 2012.

Lansiti, M., & Richards, G. L. (2011). *Economic Impact of Cloud Computing White Paper*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1875893

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). *SP 500-292: NIST Cloud Computing Reference Architecture*. Gaithersburg, MD: National Institute of Standards and Technology - Information Technology Laboratory. Retrieved from http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

Mahowald, R. P., & Sullivan, C. G. (2012). *Worldwide SaaS and Cloud Software 2012–2016 Forecast and 2011 Vendor Shares*: International Data Corporation

Malone, T. W., & Crowston, K. (1994). The interdisciplinary study of coordination. *ACM Comput. Surv., 26*(1), 87-119. doi: 10.1145/174666.174668

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing — The business perspective. *Decision Support Systems, 51*(1), 176-189. doi: http://dx.doi.org/10.1016/j.dss.2010.12.006

Mell, P., & Grance, T. (2009). *SP 800-145: The NIST Definition of Cloud Computing*. Gaithersburg, MD: National Institute of Standards and Technology - Information Technology Laboratory. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Mingers, J. (2001). Combining IS research methods: towards a pluralist methodology. *Information systems research, 12*(3), 240-259.

Mousavi, P., Marjanovic, O., & Hallikainen, P. (2012). *Disaster Recovery – The Process Management Perspective*. Paper presented at the PACIS 2012 Proceedings. Paper 67.

Najjar, W., & Gaudiot, J. L. (1990). Network resilience: A measure of network fault tolerance. *Computers, IEEE Transactions on, 39*(2), 174-181.

Nunamaker, J., Chen, M., & Purdin, T. D. M. (1991). Systems Development in Information Systems Research. *Journal of Management Information Systems, 7*(3), 89-106.

Oh, L. B., & Teo, H. H. (2006). The Impacts of Information Technology and Managerial Proactiveness in Building Net-Enabled Organizational Resilience. *The Transfer and Diffusion of Information Technology for Organizational Resilience*, 33-50.
Paton, D., & Johnston, D. (2001). Disasters and communities: vulnerability, resilience and preparedness. *Disaster Prevention and Management, 10*(4), 270-277.
Post, G. V., & Diltz, J. D. (1986). A Stochastic Dominance Approach to Risk Analysis of Computer Systems [Article]. *MIS Quarterly, 10*(4), 363-375.
Riolli, L., & Savicki, V. (2003). Information system organizational resilience. *Omega, 31*(3), 227-233.
Saya, S., Pee, L. G., & Kankanhalli, A. (2010). *The impact of institutional influences on perceived technological characteristics and real options in cloud computing adoption.* Paper presented at the International Conference On Information Systems (ICIS).
Shao, B. B. M. (2005). Optimal redundancy allocation for information technology disaster recovery in the network economy. *Dependable and Secure Computing, IEEE Transactions on, 2*(3), 262-267. doi: 10.1109/tdsc.2005.38
Stephenson, A. V. (2010). *Benchmarking the Resilience of Organisations.* Doctor of Philosophy, University of Canterbury, Christchurch.
Tierney, K. J. (2003). Conceptualizing and measuring organizational and community resilience: lessons from the emergency response following the September 11, 2001 attack on the World Trade Center.
Toomer, L. G. D. (2011). *FISMA compliance and cloud computing*. Paper presented at the Proceedings of the 2011 Information Security Curriculum Development Conference, Kennesaw, Georgia.
Undheim, A., Chilwan, A., & Heegaard, P. (2011). *Differentiated Availability in Cloud Computing SLAs.* Paper presented at the 2011 12th IEEE/ACM International Conference on Grid Computing (GRID)
Van de Walle, B., & Rutkowski, A.-F. (2006). A fuzzy decision support system for IT Service Continuity threat assessment. *Decision Support Systems, 42*(3), 1931-1943. doi: 10.1016/j.dss.2006.05.002
Weick, K. E., & Sutcliffe, K. M. (2001). Managing the Unexpected: Assuring high performance in an age of complexity. 2001. *University of Michigan Business School Management Series*.
Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. *Crisis management, 3*, 81-123.
Wilson, R. L. (2010). *Organizational Resilience Models Applied to Companies in Bankruptcy.* Doctor of Management, University of Maryland University College, United States -- Maryland. Retrieved from http://proquest.umi.com/pqdlink?did=2184332881&Fmt=7&clientI%20d=79356&RQT=309&VName=PQD
Woods, D. D., & Wreathall, J. (2008). Stress-strain plots as a basis for assessing system resilience. *Resilience Engineering: Remaining Sensitive to the Possibility of Failure*, 143-158.
World Economic Forum, & INSEAD. (2012). *The Global information Technology Report 2012: Living in a Hyperconnected World*. Retrieved from http://www3.weforum.org/docs/Global_IT_Report_2012.pdf
Yang, H., & Tate, M. (2012). A Descriptive Literature Review and Classification of Cloud Computing Research. *Communications of the Association for Information Systems, 31*(1), 2.
Zobel, C. W. (2011). Representing perceived tradeoffs in defining disaster resilience. *Decision Support Systems, 50*(2), 394-403. doi: 10.1016/j.dss.2010.10.001
Zobel, C. W., & Khansa, L. (2012). Quantifying Cyberinfrastructure Resilience against Multi-Event Attacks [Article]. *Decision Sciences, 43*(4), 687-710. doi: 10.1111/j.1540-5915.2012.00364.x